1   1.   A system to enhance safety of computer file distribution comprising:

2   (1) a computer network;

3   (2) a server computer connected to said computer network;

4   (3) one or more electronic records stored in said server computer wherein each record:

5   (a) contains information about a particular file, and

6   (b) can be retrieved when a hash value computed from said particular file using a

7   one-way hash function is presented to said server computer;

8   (4) at least one user terminal also coupled to the computer network, the user terminal

9   operable to compute the hash value of a file using said one-way hash function, and then

10 use this hash value to retrieve from said server computer the electronic record that

11 contains information about the file.

1   2.   A system to enhance safety of computer file distribution comprising:

2   (1) a computer network;

3   (2) a server computer connected to said computer network;

4   (3) one or more electronic records stored in said server computer wherein each record:

5   (a) includes information about a particular file and is indexed by a hash value

6   computed from the particular file;

7   (4) at least one user terminal connected to the computer network, the user terminal

8   operable to verify the authenticity of a particular file including

9   (a) computing the hash value of the particular file; and

10   (b) retrieving from the server computer the electronic record that contains

11 information about the particular file including submitting the computed hash to the server

12 computer.

1   3.   The system of claim 2 wherein the server computer is operable to hash using a

2   one-way hashing function the particular file and store the hash value in the associated

3   record.

1

1   4.   The system of claim 2 wherein the electronic records include a signature produced

2   by an authenticating agent associated with the particular file and wherein the step of

3   retrieving the electronic record includes retrieving the signature.

1

1   5.   The system of claim 4 wherein the authenticating agent is the author of the

2   particular file.

1

1   6.   The system of claim 2 wherein the electronic records include signature data

2   produced when validating a signature associated with the particular file and wherein the

3   step of retrieving the electronic record includes retrieving the signature data.

1   7.   The system of claim 2 wherein the particular file is a computer program.

1   8.   The system of claim 2 wherein the particular file is a data file.

1   9.   A system to enhance safety of computer file distribution over a computer network

2   comprising:

3   a server computer connected to the computer network and accessible by computer

4   network clients, the server computer including

5   one or more electronic records wherein each electronic record includes

6   information about a particular file and is indexed by a hash value computed from

7   the particular file; and

8   means for responding to client requests for information concerning a first

9   file, the client requests including a hash value computed from the first file, the

10   means for responding operable to retrieve an appropriate electronic record

11   associated with the first file and forward the information to a requesting client

12   computer.

1   10.   A system to enhance safety of computer file distribution over a computer network

2   comprising:

3   at least one user terminal connected to the computer network, the user terminal

4   operable to verify the authenticity of a particular file including

5   (a) computing the hash value of the particular file; and

6   (b) retrieving from a server computer an electronic record that contains

7   information about the particular file including submitting the computed hash to the server

8   computer.

1   11.   The system of claim 8 wherein the user terminal is operable to display the

2   information to the user terminal operator.

1   12.   A method for enhancing safety of computer file distribution comprising:

2   (1) storing one or more electronic records in a server computer wherein each

3   electronic record:

4   (a) includes information about a particular file and is indexed by a hash

5   value computed from the particular file;

6   (2) identifying a first file for authentication;

7   (3) computing the hash value of the first file; and

8   (4) retrieving from the server computer the electronic record that contains

9   information about the first file including submitting the computed hash to the server

10   computer.